COPY

Federal Aviation Administration

Memorandum

Date: JUN 14 2006

From: David Bowen, Assistant Administrator for Information Services and Chief Information Officer, AIO-1

To: Management Board

Prepared by: Mark T. Powell, Chief Technical Officer, ARD-1

Subject: Internet Protocol Version 6 (IPv6) Guidance

The purpose of this memorandum is to establish the Internet Protocol Version 6 (IPv6) guidance for the Federal Aviation Administration (FAA). This guidance will promote compliance with the attached documents: Department of Transportation's (DOT) IPv6 guidance memorandum, dated October 4, 2005, entitled DOT's Transition Planning for Internet Protocol Version 6 (IPv6); DOT's guidance memorandum, dated October 1, 2004, Guidelines for Information Technology (IT) Purchases; and the Office of Management and Budget's (OMB) guidance memorandum dated August 2, 2005, Transition Planning for Internet Protocol Version 6 (IPv6).

Internet Protocol (IP) is the "language" and set of rules computers use to talk to each other over the Internet. The most common protocol in use today, Internet Protocol Version 4 (IPv4), provides the world with only four billion IP addresses, inherently limiting the number of devices that can be given a unique, globally routable address on the Internet. The emergence of IPv6 provides the world with an almost unlimited number of available IP addresses and is essential to the continued growth of the Internet and development of new applications leveraging mobile Internet connectivity.

In August 2005, the OMB established the goal of enabling all Federal government agency network backbones to support the next generation of the IPv6 by June 30, 2008. The FAA transition will be performed using a "core out" strategy beginning with the WAN and facility backbones. In order to meet the June 2008 OMB deadline, the backbone's routers, switches, firewalls, intrusion detection systems, and network management systems must be made IPv6 compatible.

However, to completely transition the FAA to IPv6 will require replacement or upgrading of all workstations, host computers, and application software. The full transition will be expensive. However, the cost issue is mitigated by the fact that a full transition to IPv6 is expected to take

many years, and most of today's equipment will have been scrapped long before IPv6 takes over and IPv4 is permanently retired.

To facilitate this transition, it is the responsibility of the staff offices and lines of business to ensure that all future information technology procurements can use both IPv4 and IPv6 or uses native IPv6 protocol for communication with the FAA networks. The procurement of IPv6 compatible IT will allow the FAA to accomplish the transition to IPv6 through technology refresh cycles and spread the overall cost of this transition over a number of years. Requests for waivers to this policy will be reviewed and approved by the FAA CIO and forwarded to the DOT OCIO for final approval.

If you have any questions, please do not hesitate to call me on x34570 or have a member of your staff contact Hal Pierson on x58153.

Attachments
1) DOT's Transition Planning for Internet Protocol Version 6 (IPv6)
2) Guidelines for Information Technology (IT) Purchases
3) Transition Planning for Internet Protocol Version 6 (IPv6)

U.S. Department of Transportation
Office of the Secretary of Transportation

400 Seventh St., S.W.
Washington, D.C. 20590

OCT -1 2004

MEMORANDUM TO: Departmental Officers
Heads of Operating Administrations

FROM: Daniel P. Matthews
DOT Chief Information Officer, S-80

Vincent T. Taylor
Deputy Chief Acquisition Officer, M-1

SUBJECT: Guidelines for Information Technology (IT) Purchases

PURPOSE

The purpose of this memorandum is to establish guidelines for the purchase of IT products/services during the transition to the standard IT products/services in the DOT Technical Reference Model (TRM) and the phased implementation to a DOT Common Operating Environment (COE).

REFERENCES

Clinger-Cohen Act of 1996, Public Law 104-106, February 10, 1996.
Office of Management and Budget Circular A-130, Management of Federal Information Resources, November 30, 2000.
"DOT Information Technology Services Consolidation" memorandum from the DOT Chief of Staff dated October 14, 2003.
DOT Order 1350.2, "Departmental Information Resources Management Manual (DIRMM)".

SCOPE

The memorandum applies to all Operating Administrations (OAs) migrating to the DOT COE, excluding the Federal Aviation Administration (FAA).

The requirements in this memorandum are not applicable to the FAA's National Airspace System (NAS) architecture.

Although express language contained in 49 U.S.C. 106, 40110, 40121 allows for differing FAA procurement language, the DOT Chief Information Officer (CIO) and the

FAA CIO have agreed to implement these requirements for the FAA administrative network, where practical and where consistent with 49 U.S.C. 106, 40110, 40121.

BACKGROUND

Each year DOT spends a large portion of its discretionary budget on IT resources, such as computer hardware and software (including licenses), and on maintenance, training and support services for these investments. As required by the Clinger Cohen Act, the Office of Management and Budget, and at the direction of the Secretary of Transportation, the OA CIOs and the DOT CIO have been working together to identify the IT resources currently in place throughout the Department. This process has resulted in the establishment of a baseline IT architecture for the Department. Numerous commonalities were identified in this baseline, and the Department's Architecture Review Board (ARB), as chartered by Chapter 1 of the DIRMM, is in the process of identifying enterprise wide solutions to create efficiencies and reduce redundancies while meeting DOT business requirements.

In addition to identifying current IT resources, DOT has established an Information Technology Task Force (ITTF) and several newly formed IT Commodity Councils to pursue innovative and cost effective means to implement a modernized, standards-based COE that will be implemented throughout DOT in a phased approach from FY 2005-FY 2007. The implementation of this target COE will result in: An interoperable, standards-based IT infrastructure; the ability to implement Enterprise Licensing Agreements to reduce DOT's total cost of ownership of IT resources; and enhanced security of the DOT IT infrastructure. The scope of the ITTF covers: network services; telecommunications services; IT Security; desktop management services; hosting concepts; directory & messaging; service desk; records management; migration issues; physical/structural details; typical employee move process; and, network printers, copiers and fax.

IMPLEMENTATION REQUIREMENTS

Effective October 1, 2004, all commercial software, hardware and telecommunications being procured by contract (including through subcontracts), purchase order, task order (including GSA Schedules), small purchase, purchase card or otherwise, are required to be approved in advance by the OA CIO (or their designated representative). The OA CIO is responsible for ensuring that the requested IT products/services are in compliance with the standards in the DOT TRM and COE.

WAIVERS

Waivers to this memorandum will only be authorized by the DOT CIO, or appropriate designee, after consideration of the recommendation by the DOT ARB.

POINTS OF CONTACT

The points of contact for these guidelines are Darren Ash, OCIO at (202) 366-8973, and Kathy Espenshade, OSPE at (202) 366-4276.

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

M-05-22

August 2, 2005

MEMORANDUM FOR THE CHIEF INFORMATION OFFICERS

FROM: Karen S. Evans
Administrator
Office of E-Government and Information Technology

SUBJECT: Transition Planning for Internet Protocol Version 6 (IPv6)

As I stated in my testimony of June 29, 2005, before the House Committee on Government Reform, we have set June 2008 as the date by which all agencies' infrastructure (network backbones) must be using IPv6 and agency networks must interface with this infrastructure. This memorandum and its attachments provide guidance to the agencies to ensure an orderly and secure transition from Internet Protocol Version 4 (IPv4) to Version 6 (IPv6). Since the Internet Protocol is core to an agency's IT infrastructure, beginning in February, 2006 OMB will use the Enterprise Architecture Assessment Framework to evaluate agency IPv6 transition planning and progress, IP device inventory completeness, and impact analysis thoroughness.

Recent reports from the Government Accountability Office (GAO) and Department of Commerce's National Telecommunications and Information Administration (NTIA) discuss the benefits, complexity, costs, and risks organizations may encounter during the transition to IPv6. Additionally, the Department of Homeland Security's US-CERT has recently issued an advisory of security issues concerning IPv6. You should review these reports and the advisory to familiarize yourselves with the transition issues and ensure that risks are appropriately mitigated during your transition so the benefits are fully realized.[1]

What must agencies do and by when?

Following the guidance in the attachments to this memorandum, agencies must take the following actions by:

November 15, 2005

- Assign an official to lead and coordinate agency planning,
- Complete an inventory of existing routers, switches, and hardware firewalls (see Attachment A for details);

[1] References may be found at http://www.gao.gov/new.items/d05471.pdf, and http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/. The IPv6 vulnerability advisory from US-CERT was distributed via the Federal CIO Council and Small Agency Council list on April 5, 2005 and may be obtained from the secure US-CERT Portal.

- Begin an inventory of all other existing IP compliant devices and technologies not captured in the first inventory (see Attachment A for details); and
- Begin impact analysis to determine fiscal and operational impacts and risks of migrating to IPv6 (see Attachment B for details).

February 2006

- Using the guidance issued by Chief Information Officers Council Architecture and Infrastructure Committee (see below), address each of the elements in Attachment C in your agency's IPv6 transition plan and provide the completed IPv6 transition plan as part of the agency's Enterprise Architecture (EA) submission to OMB. Additional guidance on your agency's EA submission will be forthcoming.
- Provide a progress report on the inventory and impact analysis, as part of the agency's Enterprise Architecture (EA) submission to OMB. Additional guidance on your agency's EA submission will be forthcoming.

June 30, 2006

- Complete inventory of existing IP compliant devices and technologies not captured in first inventory, and
- Complete impact analysis of fiscal and operational impacts and risks.

June 30, 2008

- All agency infrastructures (network backbones) must be using IPv6[2] and agency networks must interface with this infrastructure. Agencies will include progress reports on meeting this target date as part of their EA transition strategy.

Selecting Products and Capabilities

To avoid unnecessary costs in the future, you should, to the maximum extent practicable, ensure that all new IT procurements are IPv6 compliant. Any exceptions to the use of IPv6 require the agency's CIO to give advance, written approval. An IPv6 compliant product or system must be able to receive, process, and transmit or forward (as appropriate) IPv6 packets and should interoperate with other systems and protocols in both IPv4 and IPv6 modes of operation. Specifically, any new IP product or system developed, acquired, or produced must:

- Interoperate with both IPv6 and IPv4 systems and products,
- If not initially compliant, provide a migration path and commitment to upgrade to IPv6 for all application and product features by June 2008, and
- Have available contractor/vendor IPv6 technical support for development and implementation and fielded product management.

[2] Meaning the network backbone is either operating a dual stack network core or it is operating in a pure IPv6 mode, i.e., IPv6-compliant and configured to carry operational IPv6 traffic.

The National Institute for Standards and Technology (NIST) will develop, as necessary, a standard to address IPv6 compliance for the Federal government. Additionally, as necessary, the General Services Administration and the Federal Acquisition Regulation Council will develop a suitable FAR amendment for use by all agencies.

Additional Guidance

The Chief Information Officers Council Architecture and Infrastructure Committee will develop additional IPv6 transition guidance for the agencies. The Committee anticipates completing this guidance by November 15, 2005, and will address each of the elements identified in Attachment C.

If you have questions regarding Attachment C, please contact Richard Burk at 202-395-0379. For questions on Attachments A and B, please contact Lewis Oleinick at 202-395-7188 or oleinick@omb.eop.gov.

Attachments

Attachment A: Agency IPv6 Inventory Guidance

Agencies must first conduct an inventory of existing IP-aware switches, routers, and hardware firewalls. The inventory should be conducted per "investment" as defined in OMB Circular A-11, section 53. This first inventory must be reported to OMB no later than November 15, 2005.

Agencies also must provide a second inventory of all IP compliant devices and technologies not captured by the first inventory. Agencies will provide a progress report as part of their February 2006 EA submission to OMB and as otherwise requested. This inventory must be completed and reported to OMB no later than June 30, 2006.

Both inventories should include the following data elements for each device/technology:

IPv6 Transition Checklist			
1. Investment (Name)			
Investment Name:		Investment BY06 UPI:	
Agency:		Sub-Agency:	
Program Manager:		Phone: Email:	
Prime Support Contractor:			
2. Investment Information			
a. Investment Description:			
Number of Distinct Types of Applications/Devices:		Percent of Applications/Devices IPv6 Compliant:	
Number of Distributed Sites Associated with this Investment			
3. Identify Applications or Devices used within this investment: (Add more lines as required, see Type Code legend below) - Additional details are required for complete inventory at the bottom of this report.			

Application/Device Name (Acronym)	Purpose	Type	Manufacturer/Vendor Name

Type Code Legend:

G = Government Off-the-Shelf | **C** = Commercial Off-the-Shelf | **MC** = COTS Modified by Government Contract but still available to the public

S = Shareware | **F** = Freeware

RT = Router Device | **FD** = Firewall Device | **SW** = Switch Device

AD = Authentication Device | **OD** = Other Device | **VD** = VPN/Remote Access Device available to the public.

HD = Host Device | **CD** = Client Device

4. Identify Applications or Devices that are not IPv6 compliant

Application/Device Name (Acronym)	Describe dependence on IPv4	Impact (see Legend)	IPv6 Compliant Date

Impact Code Legend:

Legacy = App/Device will be replaced before 2008 and will not transition. **Mod** = Will be modified by date identified

Upgrade = New IPv6 compliant version will be implemented by date identified guidance in **Waiver** = Waiver will be submitted per Transition Plan

5. Identify reliance on IPv4:

a. Define how IPv4 is implemented preventing IPv6 capability: (Database fields; hard-coded addressing; proprietary protocol implementation; IPv4 loopback addresses; reliance on non-IPv6 OS, COTS, or GOTS)	
b. Identify the amount of IPv4 address space used by the investment in terms of approximate CIDR address blocks, e.g. /20, /24, etc.	

6. Technical impact of transition to IPv6:

a. Describe what needs to be done to achieve initial dual stack capability and/or full transition to IPv6.	
b. Describe IPv6 characteristics that will or should be leveraged as part of the system's architecture (i.e. stacked headers, site/link local addressing, mobile IPv6, IPSec, unicast/multicast/anycast, stateless autoconfiguration).	

7. Dependencies:

a. Describe technical dependencies that will impact the IPv6 implementation, i.e. processor or memory constraints, APIs, etc.	
b. Describe logistical dependencies external to your system, i.e. interrelated programs (C2PC, TDN, etc.) Upper Layer Protocols and applications.	

8. Programmatic impact(s):

a. Schedule for systems to be dual-stack and full IPv6 compliant using current Development Schedule. Include deployment, fielding, upgrade, and retrofit milestones.	
(1) Cost schedule – list currently budgeted, such as for tech refresh or upgrade, and additional funding required (deficiency) for each FY to achieve initial and objective IPv6 capabilities in 8a. EXAMPLE: FY07 $20K($5K), FY08 $8K($0)	
b. Accelerated schedule for systems to be dual-stack and full IPv6 compliant if current Development Schedule does not meet the goal of IPv6 compliant by 2008. Include deployment, fielding, upgrade, and retrofit milestones.	
(1) Cost schedule – list currently budgeted, such as for tech refresh or upgrade, and additional funding required (deficiency) for each FY to achieve initial and objective IPv6 capabilities in 8b. EXAMPLE: FY07 $20K($5K), FY08 $8K($0)	

9. Define technical and programmatic risks.
10. Define Risk Mitigation Strategy for items identified in block 9.

11. Can this investment or the systems in the investment become a representative “early adopter”? (Yes / No)	

12. Recommendations: (Enter any comments or ideas you have that have a bearing on this initiative)

Application and Device Inventory

(Additional details continued from question #3 above)

Application/Device Name (Acronym)	Version/ OS	Device ID/ Serial number	Cost (000s)	Device Capabilities (IPv4,IPv6, dual stack)	For Firewall Devices: Does Device have the ability to monitor tunneled IPv6 traffic (Type 41 Packets) and conduct Deep Packet Inspection (Yes / No)	Supported Standards	Manufacturer Upgrade Plan	Technical Refresh Date	Device Security Level/Criticality	Known Issues with Device

Attachment B: Impact Analysis

By November 15, 2005, begin an impact analysis as described below, report on progress as part of the February 2006 agency EA submission to OMB and as otherwise requested by OMB. The results of this impact analysis must be reported to OMB no later than June 30, 2006 and must include both cost and risk elements as described in OMB Circular A-11.

Cost estimate should include:

1. Planning
2. Infrastructure Acquisition (above and beyond normal expenditures)
3. Training
4. Risk mitigation cost

Risk Analysis should consider:

1. Schedule
2. Technical obsolescence
3. Feasibility
4. Reliability of systems
5. Dependencies and interoperability issues
6. Surety (asset protection) considerations
7. Risk of creating a monopoly for future procurements
8. Capability of agency to manage the investment
9. Overall risk of investment failure
10. Organizational and change management
11. Business
12. Data/info
13. Technology
14. Strategic
15. Security
16. Privacy
17. Project resources
18. Human capital

Attachment C: Transition Activities (Notional Summary of CIO Council Guidance)

The CIO Council will develop additional transition guidance as necessary covering the following actions. To the extent agencies can address these actions now, they should do so. Beginning February 2006, agencies' transition activity will be evaluated using OMB's Enterprise Architecture Assessment Framework:

- Conduct a requirements analysis to identify current scope of IPv6 within an agency, current challenges using IPv4, and target requirements.
- Develop a sequencing plan for IPv6 implementation, integrated with your agency Enterprise Architecture.
- Develop IPv6-related policies and enforcement mechanisms.
- Develop training material for stakeholders.
- Develop and implement a test plan for IPv6 compatibility/interoperability.
- Deploy IPv6 using a phased approach.
- Maintain and monitor networks.
- Update IPv6 requirements and target architecture on an ongoing basis.